

IN THE CLAIMS:

Claim 1 (Previously Cancelled)

- I
- 1 2. (Previously Presented) The system of claim 6, wherein the
2 communications engine uses SSL to create a secure
3 communications link with the client.
- 1 3. (Previously Presented) The system of claim 6, wherein the
2 communications engine negotiates an encryption protocol
3 for transferring messages to and from the client.
- 1 4. (Previously Presented) The system of claim 6, wherein the
2 communications engine uses public key certificates for
3 transferring messages to and from the client.
- 1 5. (Previously Presented) The system of claim 6, wherein the
2 security services use public key certificates to
3 authenticate a user of the client to determine the user
4 privileges.
- 1 6. (Previously Presented) A system on a server computer
2 system, comprising:
3 a communications engine for establishing a communications
4 link with a client;
5 security services coupled to the communications engine
6 for presenting to a user of the client a plurality
7 of user authentication protocol options, each user
8 authentication protocol option having a particular
9 level of authentication associated with it, for
10 authenticating the user according to at least one

11 user authentication protocol and for determining
12 user privileges based on the identity of the user
13 and the level of authentication;
14 a web server for presenting a set of available services
15 based on the user privileges, at least one of the
16 available services requiring additional
17 authentication information to be provided before
18 access to the service is granted, and for enabling
19 the client to select a particular service from the
20 set of available services;
21 a host engine coupled to the security services and to the
22 web server for providing to the client service
23 communication code that enables communication with
24 the particular service; and
25 a keySAFE for storing keys, each key for enabling
26 communication between the client and a respective
27 service from the set of available services and
28 including all additional authentication information
29 required by the respective service for
30 authenticating the user to the respective service,
31 thereby enabling the client to access the available
32 services without storing the service communication
33 code and keys at the client or having to carry or
34 remember them.

Claim 7 (Previously Cancelled)

1 8. (Currently Presented) The system of claim 6, wherein the
2 security services use a digital signature to authenticate
3 the user to determine the user privileges.

1 9. (Previously Presented) The system of claim 6, wherein the
2 host engine forwards to the client security code for
3 enabling the client to perform a security protocol
4 recognized by the security services.

1 10. (Currently Presented) The system of claim 6, wherein one
2 of the available services is secured by a firewall and
3 one of the keys includes the additional authentication
4 information to enable communication through the firewall.

1 11. (Previously Presented) The system of claim 6, further
2 comprising a firewall for protecting the system.

1 12. (Previously Presented) The system of claim 6, wherein one
2 of the keys includes an address identifying the location
3 of the selected service.

1 13. (Previously Presented) The system of claim 6, wherein the
2 code uses a key to provide to the client a direct
3 connection with the selected service.

1 14. (Previously Presented) The system of claim 6, further
2 comprising a proxy for communicating with the selected
3 service, and wherein the code enables the client to
4 communicate with the proxy and one of the keys enables
5 the proxy to locate the selected service.

Claim 15 (Previously Cancelled)

10 determining user privileges based on the identity of a
11 user and the level of authentication;
12 presenting a set of available services based on the user
13 privileges, at least one of the available services
14 requiring additional authentication information to
15 be provided before access to the service is
16 granted;
17 enabling the client to select a particular service from a
18 set of available services;
19 providing to the client service communication code that
20 enables communication with the particular service;
21 and
22 retrieving a key from a set of keys, each key
23 corresponding to a respective service from the set
24 of available services, the retrieved key for
25 enabling communication between the client and the
26 particular service and including all additional
27 authentication information required by the
28 respective service for authenticating the user to
29 the respective service, thereby enabling the client
30 to access the available services without storing
31 the service communication code and keys at the
32 client or having to carry or remember them.

1 Claim 21 (Previously Cancelled)

1 22. (Previously Presented) The method of claim 20, wherein
2 determining user privileges includes the step of using a
3 digital signature to authenticate the user.

1 16. (Previously Presented) The method of claim 20, wherein
2 establishing a communications link includes the step of
3 using SSL to create a secure communications link with the
4 client.

1 17. (Previously Presented) The method of claim 20, wherein
2 establishing a communications link includes the step of
3 negotiating an encryption protocol for transferring
4 messages to and from the client.

I
1 18. (Previously Presented) The method of claim 20, wherein
2 establishing a communications link includes the step of
3 using public key certificates for transferring messages
4 to and from the client.

1 19. (Previously Presented) The method of claim 20, wherein
2 determining user privileges includes the step of using
3 public key certificates to authenticate a user of the
4 client.

1 20. (Previously Presented) A computer-based method
2 comprising:
3 establishing a communications link with a client;
4 presenting to a user of the client a plurality of user
5 authentication protocol options, each user
6 authentication protocol option having a particular
7 level of authentication associated with it;
8 authenticating the user according to at least one user
9 authentication protocol option;

1 23. (Previously Presented) The method of claim 20, wherein
2 establishing a communications link includes forwarding to
3 the client security code for enabling the client to
4 perform a recognized security protocol.

1 24. (Previously Presented) The method of claim 20, further
2 comprising the step of using one of the keys to
3 communicate through a firewall to the selected service.

I 1 25. (Previously Presented) The method of claim 20, wherein
2 the method is performed by a server and further
3 comprising using a firewall to protect the server.

1 26. (Previously Presented) The method of claim 20, wherein
2 one of the keys includes an address identifying the
3 location of the selected service.

1 27. (Previously Presented) The method of claim 20, wherein
2 providing includes the step of providing to the client a
3 direct connection with the service.

1 28. (Previously Presented) The method of claim 20, further
2 comprising using a proxy to communicate with the service,
3 and wherein providing includes enabling the client to
4 communicate with the proxy.

1 29. (Currently Amended) A system on a server computer system,
2 comprising:
3 means for establishing a communications link with a
4 client;

5 means for presenting to a user of the client a plurality
6 of user authentication protocol options, each user
7 authentication protocol option having a particular
8 level of authentication; ~~associated with it,~~
9 means for authenticating the user according to at least
10 one user authentication ~~protocol,~~ and protocol;
11 means for determining user privileges based on the
12 identity of a user and the level of authentication;
13 I means for presenting a set of available services based on
14 the user privileges, at least on of the available
15 services requiring additional authentication
16 information to be provided before granting access
17 to the ~~service is granted,~~ and service;
18 means for enabling the client to select a particular
19 service from a set of available services;
20 means for providing to the client service communication
21 code that enables communication with the particular
22 service; and
23 means for retrieving a key from a set of keys, each key
24 corresponding to a respective service from the set
25 of available services, the retrieved key for
26 enabling communication between the client and the
27 particular service and including all additional
28 authentication information required by the
29 respective service for authenticating the user to
30 the respective service, thereby enabling the client
31 to access the available services without storing
32 the service communication code and keys at the
33 client.

I 30. (Previously Presented) A computer-based storage medium
storing a program for causing a computer to perform the
steps of:
establishing a communications link with a client;
presenting to a user of the client a plurality of user
authentication protocol options, each user
authentication protocol option having a particular
level of authentication associated with it;
authenticating the user according to at least one user
authentication protocol option;
determining user privileges based on the identity of a
user and the level of authentication;
presenting a set of available services based on the user
privileges, at least one of the available services
requiring additional authentication information to
be provided before access to the service is
granted;
enabling the client to select a particular service from a
set of available services;
providing to the client service communication code that
enables communication with the particular service;
and
retrieving a key from a set of keys, each key
corresponding to a respective service from the set
of available services, the retrieved key for
enabling communication between the client and the
particular service and including all additional
authentication information required by the
respective service for authenticating the user to

30 the respective service, thereby enabling the client
31 to access the available services without storing
32 the service communication code and keys at the
33 client or having to carry or remember them.

1 Claim 31 (Previously Cancelled)

I 1 32. (Currently Amended) A method, comprising:
2 receiving, from a client, as an advance communication,
3 security information corresponding to one or more
4 secured network services;
5 storing the security information at a location remote
6 from the client;
7 receiving a user ~~client~~ request from a user ~~the client~~ to
8 access a secured network service; and
9 using the stored security information to enable the user
10 ~~client~~ access to the secured network service
11 without requiring the user ~~client~~ to supply the
12 stored security information.

1 33. (Previously Presented) A method according to claim 32,
2 wherein the security information includes one or more
3 keys corresponding to respective ones of the secured
4 network services.

1 34. (Currently Amended) A method according to claim ~~32~~ 33,
2 wherein at least one of the keys includes a certificate
3 for accessing at least one of the secured network
4 services.

1 35. (Currently Amended) A method according to claim 32,
2 further comprising determining user ~~elient~~ privileges of
3 the user ~~elient~~, and wherein the using the stored
4 security information is provided if the privileges
5 correspond to privilege requirements of the secured
6 network service.

I 1 36. (Currently Amended) A method according to claim 32,
2 further comprising determining user ~~elient~~ privileges of
3 the user ~~elient~~ and enabling the user ~~elient~~ to select a
4 service from ones of the secured network services
5 corresponding to the determined user ~~elient~~ privileges.

1 37. (Currently Amended) A system, comprising:
2 means for receiving, from a client, as an advance
3 communication, security information corresponding
4 to one or more secured network services;
5 means for storing the security information at a location
6 remote from the client;
7 means for receiving a user ~~elient~~ request from a user ~~the~~
8 ~~elient~~ to access a secured network service; and
9 means for using the stored security information to enable
10 the user ~~elient~~ access to the secured network
11 service without requiring the user ~~elient~~ to supply
12 the stored security information.

I 1 38. (Currently Amended) A computer-readable storage medium
2 storing program code for causing a computer to perform
3 the steps of:
4 receiving, from a client, as an advance communication,
5 security information corresponding to one or more
6 secured network services;
7 storing the security information at a location remote
8 from the client;
9 receiving a user ~~elient~~ request from a user ~~the client~~ to
10 access a secured network service; and
11 using the stored security information to enable the user
12 ~~elient~~ access to the secured network service
13 without requiring the user ~~elient~~ to supply the
14 stored security information.

1 39. (Previously Presented) A server computer system,
2 comprising:
3 a communications engine for establishing a communications
4 link with a client;
5 security services coupled to the communications engine
6 for presenting a user of the client a plurality of
7 user authentication protocol options, each user
8 authentication protocol option having a particular
9 level of authentication associated with it, for
10 authenticating the user according to at least one
11 user authentication protocol and for determining
12 user privileges based on the identity of the user
13 and the level of authentication; and
14 a web server for presenting information to the user based
15 on the user privileges.